Message

From:	brian@atencoin.com [brian@atencoin.com]
Sent:	10/15/2015 8:24:09 AM
To:	[redacted]
Subject:	Fwd: Aten Coin vs Bitcoin
Attachments:	Comparison between Aten Coin & Bitcoin.pdf

-------- Original Message --------
Subject: Aten Coin vs Bitcoin
Date: 2015-10-14 11:09
From: Marcus Monex [redacted]
To: Black Gold <[redacted]>, "brian@atencoin.com" <brian@atencoin.com>, "sales@atencoin.com" <sales@atencoin.com>
Cc: Patti NAC Office <bookkeeper@atencoin.com>

Good Read

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
TRIAL EXHIBIT 0811
CASE NO.: CR 20-249 RS
DATE ENTERED_________
BY____________________
DEPUTY CLERK

Comparison between Aten Coin & Bitcoin

NAC Foundation

1 October 2015

Tracing & Tracking Legal Identities of Individual Senders & Receivers

Aten Coin

- Traceable and trackable
- Public cannot trace and track legal identity of any senders and receivers
- National Aten Coin Foundation can trace and track legal identity of any senders and receivers

Justifications

- Currency address (for receiving and sending money) can only be created by registered users with verified legal identity.
  - Using privately regulated public blockchain technology (patent pending)
- Each currency address is linked to a person having legal identity stored in the Aten Coin Client database.
- Transaction can only be created by registered users with verified legal identity.
  - Using privately regulated public blockchain technology (patent pending)

Bitcoin

- Not traceable & Not trackable
- Public cannot trace and track legal identity of any senders and receivers
- Bitcoin Foundation cannot trace and track legal identity of any senders and receivers

Justifications

- Currency address can be created by anyone.
  - Based on public blockchain technology, of which no one can control who can or who cannot create receiver addresses
- Owners of individual currency addresses are anonymous.
- Transaction can be created by anyone.
  - Based on public blockchain technology

Detection & Stoppage of Suspicious Money Transactions of Individual Transactions

Aten Coin

- Detectable
  - At individual sender and receiver level
- All transactions are stoppable
  - At individual transaction level

Justifications

- Transaction can only be created by registered users with verified legal identity.
  - Using privately regulated public blockchain technology (patent pending)
- As personal identities of all senders and receivers are known, we could identify all transaction records as well as locations (IP addresses) of individual senders and receivers.
- All transactions are monitored and regulated by NAC Foundation (NAC).
- All transactions are monitored with Patriot Officer to detect suspicious transactions.
- All transactions requires NAC's signature to proceed.
- NAC first examines whether a new transaction request fulfills NAC's "non-suspicious" criteria, and only signed those non-suspicious transactions with the NAC's private key.

Bitcoin

- Partially Detectable
  - At IP address level, but <10% of the Bitcoin addresses of which locations are traceable
- Most transactions are non-stoppable
  - Can only be stoppable if one uses a Bitcoin wallet that has implemented such function.

Justifications

- By design, owners of bitcoin addresses are anonymous.
- People can only use IP addresses of the senders to trace the geographic location of the senders. By analyzing the geographic location of senders, one can identify whether there are suspicious flow of money into a specific location.
  - Only applicable to <10% of bitcoin addresses
  - Cannot identify at level of individual senders
  - Cannot identify IP addresses of receivers
  - Receivers can send the wallet.dat to another geographic location, and spend the received bitcoins at other locations to void detection of real location.
- By design, there is no control in transactions as long as the required private keys are available for signing the transactions.
- Only people who are using KYC-compliant Bitcoin wallets can be subjected to identity disclosure.
- Only those transactions which are created by using specially designed Bitcoin wallets can be suspended until the required private keys are available for signing the transactions.

EX811-004

Know-Your-Customer & Anti-Money Laundering Compliance

Aten Coin

- Yes

Justifications

- Legal identities of all senders and receivers can be identified by NAC.
- Privacy of all senders and receivers are protected because public cannot identify senders and receivers from the blockchain.
- All transactions are monitored with Patriot Officer to detect suspicious transactions.
- All suspicious transactions will be reported to the FINCEN (USA) and relevant government regulatory offices, according to the geographic location (tracing from the IP addresses) of senders and receivers.
- National Aten Coin Foundation is a service member of the American Bank Association (ABA) and compliant with various important AML and anti-criminal regulations.
  - See next page of details

Bitcoin

- No

Justifications

- By design, bitcoin transaction system is anonymous.
- An academic study (Meiklejohn S, et al. University of California, San Diego, 2013) showed that evidence of interactions between institutes could be identified by analyzing the pattern of involvements of Bitcoin addresses in empirical purchasing of goods and services.
- This approach may be able to identify illegal activities at institution level, but still not able to narrow down to a single person level. A recent academic study (Koshy P, et al. Pennsylvania State University, 2014) has shown that it is possible to map a Bitcoin address to an IP address. However, this approach is only applicable to less than 10% of the Bitcoin addresses. Therefore, it is generally believed that Bitcoin and other alternative cryptocurrencies can be used for illegal activities such as money laundering (Bryans D, Indiana Law Journal, 89 (1):441, 2014).

Aten Coins Compliant with:

a) Anti-Money Laundering (AML),

b) Counter Financing of Terrorism (CFT),

c) Anti-Fraud and Financial Crimes (AFF),

d) Office of Foreign Assets Control (OFAC),

   i. Specially Designated Nationals List (SDN)

   ii. Consolidated List (OFCL)

e) Bank Secrecy Act (BSA),

f) USA PATRIOT Act,

g) FACT Act.

h) FBI Most Wanted

i) BIS Denied Person

j) Canadian OSFI List

k) Europe HM Treasury Sanction List

l) European Union Sanctions List

m) United Nations 1267 List

Thief Resistance

Aten Coin

- Yes

Justifications

- Aten Coin achieves this at multiple levels.
- All atencoin addresses are multisignature addresses. Each address requires a private key (non-changeable) from NAC and at least one private key (non-changeable) from clients to sign transaction inputs.
- All atencoin transactions require a private key, which can be changed anytime, from NAC to sign the whole transaction. Even both the NAC's private key and client's private key of a multisignature address are being stolen. NAC can stop the atencoins being sent out from that address by not signing the whole transaction.
- When an atencoin wallet are stolen, owner of the atencoin wallet can inform NAC to stop any atencoins being sent out from a stolen wallet.
- NAC can lock atencoins stored at any atencoin addresses by not signing any transactions in which atencoins stored at those addresses are being spent.
- When atencoins are being stolen by hacking, the stolen atencoins have to be sent to at one or more receiver addresses. NAC can identify legal identifies of thieves by tracing the legal personal identities of owners of those receiver addresses.

Bitcoin

- No

Justifications

- It is well known that Bitcoin is not thief resistant.
- Exchange platforms use cold wallets to avoid hacking, but such approach achieves minimal success. For example, in February 2014, the Mt. Gox company, which was the world largest bitcoin exchange company at that time, was filed for bankruptcy protection because the company was being hacked continuously, resulting in loss of 850,000 bitcoins (worth about US$ 480 million). In December 2014, Atlanta's Bitpay got hacked for $1.8 million in bitcoin. In January 2015, the Slovenian Bitcoin exchange Bitstamp, which was the world's third largest bitcoin exchange at that time, was hacked, and less than 19,000 BTC (worth about US$ 5 million) was stolen.
- Various bitcoin wallets are being developed to achieve thief resistance, e.g. wallet using multisignature bitcoin addresses. One private key can be stored in a remote server and is only available upon a valid request (e.g. protection by fingerprint matching, a technology provided by Case Wallet Inc ,aka CryptoLabs). However, bitcoins can still be sent out from a multisignature address by stealing all required private keys.

Transaction Speed

Aten Coin

- Average time required for 1st confirmation: 32 sec (9.4 times faster than Bitcoin)
- Average time required for 6 confirmations: 332 sec (9.9 times faster than Bitcoin)

Justifications

- Average block time: 64 seconds

Bitcoin

- Average time required for 1st transaction confirmation is 300 sec (5 minutes)
- Average time required for 6 confirmations: 3300 sec (55 minutes)

Justifications

- Average block time: 600 sec

ANDRADE_DOJ_00071326

Transaction Capacity

Aten Coin

- 65 transactions per second

Justifications

- All transactions are recorded in the blockchain of Aten Coin.
- Average block time: 64 seconds
- Maximum data size per block: 1 MB
- Average 9.375 MB per 600 sec
- Hence, Aten Coin has 9.375 times more transaction capacity than Bitcoin.
- As a result, Aten Coin can handle 65 transaction per second.

Bitcoin

- 7 transactions per second (https://en.bitcoin.it/wiki/Scalability)

Justifications

- All transactions are recorded in the blockchain of Bitcoin.
- Average block time: 600 sec
- Maximum data size per block: 1 MB
- Average 1 MB per 600 sec

Security

Aten Coin

- X11
  - a more secure cryptographic algorithm compared to that of Bitcoin
- Less susceptible to 51% attack

Justifications

- X11 was originally developed by the Darkcoin team. It is a super secure hashing algorithm comprising 11 rounds of scientific hashing functions (blake, bmw, groestl, jh, keccak, skein, luffa, cubehash, shavite, simd, echo).
- Protected against security risks like SPOF (Single Point Of Failure).
- X11 can only break when all 11 hashing functions are broken by computing breakthrough.
- Transactions are recorded in new blocks generated by Proof-of-Stack (PoS), which is less susceptible to 51% attack
  - Only atencoin holders can mine atencoins.
  - It is also impossible to obtain >50% atencoins (too high cost) to perform 51% attack
  - To minimize the chance of 51% attack, NAC will keep 7 million ATENC (currently 24 million ATENC generated) for PoS.

Bitcoin

- SHA256
  - first cryptographic algorithm used for making cryptocurrency
- More susceptible to 51% attack

Justifications

- SHA256 algorithm comprise only 1 round of SHA256 hashing.
- Not protected against security risks like SPOF (Single Point Of Failure).
- Computing breakthrough that “breaks” the SHA256 hash could jeopardize the entire Bitcoin network until the network shifts through a hard fork to another cryptographic hash
- Transactions are recorded in new blocks generated by Proof-of-Work (PoW). 51% attack is possible when
  - Public has less incentive to mine bitcoins because of reduced bitcoin rewards for successful mining a new block.
  - one acquires super-computers to achieve >50% of computation power for mining bitcoins.

Cost for Maintaining Transaction Network

Aten Coin

- Extremely low operation cost

Justifications

- Compared to Bitcoin, Aten Coin's transaction network is much more economical. Aten Coin uses Proof-of-Stake (PoS) mining strategy. Only Aten Coin holders can mine Aten Coin. Therefore, Aten Coin only requires computation power from Aten Coin holders.
- Furthermore, for PoS mining, computers having low-end CPU are already sufficient.

Bitcoin

- Hugh operation cost

Justifications

- It is well known that it is extraordinary expensive to main the transaction network of Bitcoin by Proof-of-Work mining.
- The current hash rate for Bitcoin is equivalent to computation power of 35 billion i7 CPUs.

Liquidity and Value Stability

Aten Coin

- Depend on public usage
- Supported by Oil and Gas production projects

Justifications

- Aten Coin is created by NAC. Besides relying on the public demand, NAC is trying her best to ensure there is demand of atencoins in the market.
- NAC solves this problem by creating a stable market demands through joint venture business in oil well drilling.
- NAC pays Black Gold Coin International, Inc (BGCI) to promote the use of Aten Coin. BGCI is initiating joint venture oil well drilling projects. The profit from these projects will be paid to BGCI from our joint venture partners in Aten Coin. This not only creates a continuous demand of Aten Coin, but also helps maintaining its value.
- It is important to note that BGCI's joint venture partners cannot purchase atencoins from NAC, and has to obtain atencoins from exchange markets, in which the exchange rate is dictated by the public.

Bitcoin

- Depend only by public usage

Justifications

- Bitcoin is a 100% decentralized digital currency. No one has obligation to use bitcoins.
- It is well known that Bitcoin is not backed by any real assets. This makes value of bitcoin volatile.
- If no one uses bitcoins, Bitcoin's value will become zero.

Possibility of Disagreement in Future Development of a Cryptocurrency

Aten Coin

- Not possible

Justifications

- Aten Coin is not an open-source code project which is carried out by NAC.
- NAC is the central governance body of Aten Coin. Only NAC can dictate the future development of Aten Coin.
- Only NAC can change properties of Aten Coin by modifying the source code.

Bitcoin

- Possible

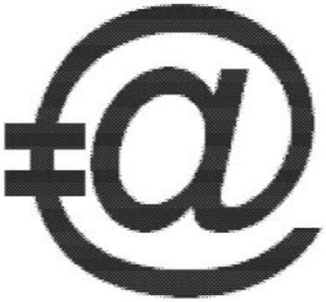
Justifications

- Bitcoin is an open-source code project.
- There is no central governance body of Bitcoin.
- Anyone who is interested in bitcoin can modify the source code. However, the new source code has to be accepted by >50% of Bitcoin network.
- As Bitcoin network is supported by computation power from the public, modifying bitcoin's source code has to be acceptable by majority of the public.
- If consensus in the public cannot be achieved and two versions of bitcoin protocols are supported by highly similar amount of computation power in the network, Bitcoin's transaction will be messed up by the presence of two blockchains operating in parallel.
- For example, the recent "Bitcoin Block Size Debate" has not yet reached consensus as of 30/9/2015.

Other comparisons

Aten Coin

- Maximum amount: 26 million
- Available supply: 19,040,748 as of 30/9/2015.
- Amount created by creator: 24 million
- Abbreviation: ATENC
- Symbol:



Bitcoin

- Maximum amount: 24 million
- Available supply: 14,674,150 as of 30/9/2015
- Amount created by creator: unknown
- Abbreviation: BTC
- Symbol:

Disclaimers – Issue of Underlying Collateral

- NAC has created 24 million atencoins. 12 million of them are being sold to the public. 5 million of the 12 million Aten Coins have been sold already.
- Black Gold Coin International (BGCI), Inc. is an Aten Coin Promotion Company. NAC and BGCI are two separate entities. NAC will pay BGCI to promote the use of Aten Coin. Proceeds from the promotion company BGCI will not be shared with Aten Coin Holders. Aten Coin does not have any underlying collateral.
- One important promotion campaign of BGCI is collaborating with stakeholders in Oil and Gas Industry on Oil and Gas production. BGCI has invested and will continue to invest in oil and gas projects as long as an Aten Coin Proceeds Agreement is signed. Aten Coin Holders do not participate in these oil and gas project profits.
- Aten Coin's Funding Agreements with their oil and gas partners provide for the oil and gas companies to share profits with BGCI in Aten Coin. The amounts paid in Aten Coin to BGCI will be obtained by the oil and gas partners from the exchanges. These ongoing coin purchases should enhance the market, since the goal of BGCI is to always have a buyer in the market place. Except for paying U.S. income taxes due from these oil and gas proceeds, BGCI intends to hold these coins in the company treasury. NAC, BGCI and their current and future associated companies do not have any obligation to purchase Aten Coin from the Aten Coin Holders. NAC, BGCI and their current and future associated companies should not be relied upon to be a source of liquidity for Aten Coin Holders and Aten Coin Holders' atencoins.